Cyber Security and the Government / Private Sector Connection

Jeffrey F. Addicott

Jeffrey F. Addicott, *Cyber Security and the Government / Private Sector Connection*, 21 Pass It On 1 (Spring 2012).

Spring 2012
Vol. 21, No. 3

pass it on

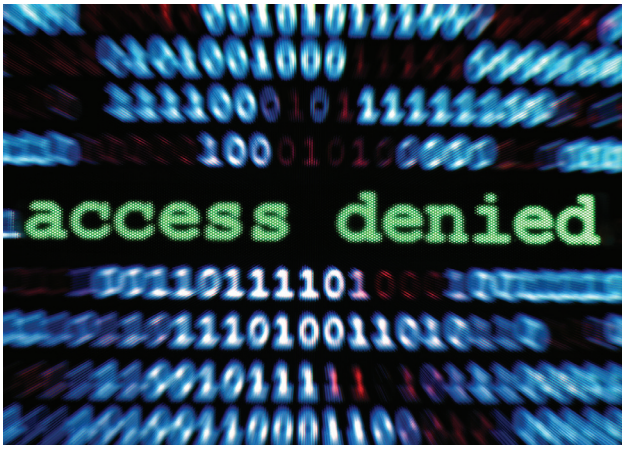
The newsletter of the American Bar Association's Government and Public Sector Lawyers Division

Cyber Security and the Government/Private Sector Connection

By Jeffrey F. Addicott

Recent escalation of alleged Chinese-based hacking of U.S. defense companies and the U.S. Chamber of Commerce, and the coordinated cyber attacks that shut down the entire nation of Estonia in 2007 illustrate the scope of the cyber security threat that exists today. Whether emanating from a terrorist organization, criminal element, severe weather incident or human error, a significant cyber disruption is very likely to affect the United States in the foreseeable future; it is naïve to think otherwise.

Despite these serious risks, most experts agree that the United States does not currently possess a sufficient cyber security framework to adequately protect cyberspace and the information it contains, processes, and transmits. In part, this is because over 85 percent of the critical infrastructure in the United States is controlled by private industry. In most instances, government cyber security standards do not apply to the civilian sector. While the government has embarked on a variety of initiatives with private and public entities to protect against the threat of cyber disruption, many legal and policy issues remain unanswered.



The greatest concern is an intentional cyber attack against the electronic control systems, e.g., the Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, or any equivalent system that regulates the operational functions of our critical infrastructure through thousands of interconnected computers, servers, routers, and switches. The centralized computer networks that monitor and control our entire critical infrastructure present tempting targets. Even a single SCADA disruption could cause enormous economic and physical damage across broad sections of the country. The impact could include massive human casualties, wide-scale economic damage, and significant disruption of national readiness for war.

However, not all disruptions of an information system's confidentiality, integrity, or availability (CIA) constitute a cyber attack. In fact, most disruptions of information systems are caused by unintentional human error and are called cyber incidents. The National Institute of Standards and Technology defines a cyber incident as:

> An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional.

Generally, there are four types of cyber attacks. First, the most common type of cyber attack is service disruption or the distributed denial of service (DDoS) attack, which aims to flood the target computer with data packets or connection requests, thereby making it unavailable to the user or, in the case of a website, unavailable to the website's visitors. DDoS attacks are often conducted utilizing "zombies"—computer systems controlled by a "master" through the utilization of "bots" or "botnets." Service disruption could directly affect any aspect of the critical infrastructure, causing regional or even global damage. A second, but related, type of cyber attack is designed to capture and then control certain elements of cyberspace in order to use them as actual weapons. This strategy was allegedly used in April, 2010 when a state-owned telecommunications company hijacked 15 percent of the internet traffic in the United

AMERICAN BAR ASSOCIATION
Government and Public Sector Lawyers Division

Tips for Practitioners

Ensure that you are familiar with the applicable state law associated with cyber issues where you practice. Many states have enacted legislation that now requires businesses to notify affected persons when a cyber security breach occurs and personal information is compromised. In addition, some states also require businesses to provide "reasonable" cyber security protections.

Ensure that you have the appropriate level of cyber security to protect the information that you store and transfer. Hiring an outside cyber security professional to evaluate your cyber security protocols and procedures is encouraged.

Understand the criminal statutes—both state and federal—related to prosecuting cyber crime.

States, which included the Pentagon's network and Secretary Gates' office. The third category of cyber attack is aimed at theft of assets from, for example, financial institutions. This activity includes not only theft, but also extortion and fraud. Finally, a cyber attack can be a conventional explosive attack on a physical structure, such as a building that houses a SCADA.

The central focus of cyber security is protection of an information system's CIA. According to the 2005 Congressional Research Service report, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, cyber security refers to:

> a set of activities and other measures intended to protect—from attack, disruption, or other threats—computers, computer networks, related hardware and devices software, and the information they contain and communicate, including software data, as well as other elements of cyberspace. The activities can include security audits, patch management, authentication procedures, access management, and so forth. They can involve, for example, examining and evaluating the strengths and vulnerabilities of the hardware and software used in the country's political and economic electronic infrastructure. They also involve detection and reaction to security events, mitigation of impacts, and recovery of affected components. Other measures can include such things as hardware and software firewalls, physical security such as hardened facilitates, and personnel training and responsibilities.

Starting with the Reagan Administration and continuing to the Obama Administration, the government's approach to cyber security has been one of cooperative engagement and not mandatory regulation. With minor exceptions, when private industry works with the government, the theme of engagement predominates all of the federal laws, executive orders and presidential directives associated with cyberspace. The National Strategy to Secure Cyberspace specifically recognizes that cyberspace constitutes "the control system of our country." In addition, the document recognizes that a comprehensive national strategy must protect against such cyber attacks which "can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life."

In May 2009, the Obama Administration released its Cyberspace Policy Review with a key recommendation centered on the engagement strategy

Editor
Laura Beliveau

Staff Editors
Katherine Mikkelson
Susan Kidd

Comments, letters to the editor and other suggestions
Editor, Government and Public Sector Lawyers Division
American Bar Association
740 15th Street, NW
Washington, DC 20005
202-662-1020

E-mail
GPSLD@americanbar.org

Visit our homepage
www.governmentlawyer.org

Reprint requests must be made in writing to copyright@americanbar.org.

Editorial Statement
Pass It On provides a forum for the discussion of issues of special concern to government and public sector lawyers. *Pass It On* is edited by members of the Government and Public Sector Lawyers Division. Publishing and editorial decisions are based on the editors' judgment of the quality of the writing, the timeliness of the article, and the potential interest to the readers of *Pass It On*. The views in *Pass It On* are those of the authors and may not reflect the official policy of the American Bar Association or the Government and Public Sector Lawyers Division. No endorsement of the views should be inferred unless specifically identified as the official policy of the American Bar Association or the Government and Public Sector Lawyers Division.

AMERICAN BAR ASSOCIATION
Government and Public Sector Lawyers Division

of improving partnerships between the private sector and the government. According to the Cyberspace Policy Review:

> Some members of the private sector continue to express concern that certain federal laws might impede full collaborative partnerships and operational information sharing between the private sector and government. For example, some in industry are concerned that the information sharing and collective planning that occurs among members of the same sector under existing partnership models might be viewed as 'collusive' or contrary to laws forbidding restraints on trade.

Cooperation between the government and the private sector is currently weak. Unfortunately, it is a hard fact that very few private companies have exhibited interest in joining the cyber security effort to the degree that the various government strategies require. Partnering the private industry with the government is imperative to an effective cyber security system. Eventually, the government may be forced to implement mandatory programs to ensure that private industry shares information and develops systems that are more secure. To date, the complacent habit of dealing only with realized threats has not imparted a sense of urgency that will ultimately be necessary to protect the cyber world. Executive Order 13249, signed in January 2010, directs agency heads to promulgate rules and procedures for the sharing of sensitive information with private sector entities and directs the Department of Defense to inspect, accredit and monitor private sector facilities where classified information is or will be used.

Senate Bill 2105 was introduced in February to strengthen computer defenses for private businesses such as banks, telecommunications, transportation, and utilities. The bill would require the Department of Homeland Security to assess the risks

Common Techniques for a Cyber Attack

Type	Description
Spamming	Sending unsolicited commercial email advertising for products, services, and websites. Spam can also be used as a delivery mechanism for malware and other cyber threats.
Phishing	A high-tech scam that frequently uses spam or pop-up messages to deceive people into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information. Internet scammers use email bait to "phish" for passwords and financial data from the sea of internet users.
Spoofing	Creating a fraudulent website to mimic an actual, well-known website run by another party. Email spoofing occurs when the sender address and other parts of an email header are altered to appear as though the email originated from a different source. Spoofing hides the origin of an email message.
Pharming	A method used by phishers to deceive users into believing that they are communicating with a legitimate website. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed website when the user types in a legitimate web address. For example, one pharming technique is to redirect users—without their knowledge—to a different website from the one they intended to access. Also, software vulnerabilities may be exploited or malware employed to redirect the user to a fraudulent website when the user types in a legitimate address.
Denial of service attack	An attack in which one user takes up so much of a shared resource that none of the resource is left for other users. Denial of service attacks compromise the availability of the resource.
Distributed denial of service	A variant of the denial of service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Viruses	A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. A virus requires human involvement (usually unwitting) to propagate.
Trojan horse	A computer program that conceals harmful code. It usually masquerades as a useful program that a user would wish to execute.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
Malware	Malicious software designed to carry out annoying or harmful actions. Malware often masquerades as useful programs or is embedded into useful programs so that users are induced into activating them. Malware can include viruses, worms, and spyware.
Spyware	Malware installed without the user's knowledge to surreptitiously track and/or transmit data to an unauthorized third party.
Botnet	A network of remotely controlled systems used to coordinate attacks and distribute malware, spam, and phishing scams. Bots (short for "robots") are programs that are covertly installed on a targeted system allowing an unauthorized user to remotely control the compromised computer for a variety of malicious purposes.

Source: GAO-07-705, June 2007

and vulnerabilities of such systems to determine which should be required to meet certain risk-based security standards. The bill envisions that DHS would work with company officials to develop performance requirements based on current industry standards. A third party assessor could be used to verify compliance. The bill also proposes information sharing between companies and the federal government with respect to threats, incidents, best practices and fixes. Whether this bill passes and will lead to closer coordination between the private and public sectors remains an unanswered question.

Professor Jeffrey F. Addicott is the Director of the Center for Terrorism Law at St. Mary's University School of Law, San Antonio, Texas. An active duty Army officer in the Judge Advocate General's Corps for twenty years (he retired in 2000 at the rank of Lieutenant Colonel), Professor Addicott spent a quarter of his career as a senior legal advisor to the United States Army's Special Forces. As an internationally recognized authority on national security law, terrorism law and human rights law, Professor Addicott lectures and participates in professional and academic organizations both in the United States and abroad, and is a frequent contributor to national and international news shows including FOX News Channel and MSNBC. Professor Addicott has published over 20 books, articles, and monographs on a variety of legal topics. Addicott's most recent book is Terrorism Law: Cases, Materials, Comments. *This article is a modified version of a chapter in the 6th edition.*

ABA MILITARY PRO BONO PROJECT

The ABA Military Pro Bono Project connects junior-enlisted, active-duty military personnel and their families to civilian attorneys who provide free representation for civil legal issues beyond the scope of services provided by military legal assistance offices. The Project accepts case referrals from military legal assistance attorneys (i.e., JAG attorneys) across the country and around the world, and connects these service members with pro bono attorneys throughout the United States. The Project also includes Operation Stand-By, through which attorneys may volunteer to provide lawyer-to-lawyer consultations to military attorneys in need of information on substantive or state-specific legal issues. For more information or to register as a volunteer with the Project, visit **www.militaryprobono.org**.

E-Discovery in Government Investigations and Criminal Litigation

April 13, 2012
Los Angeles, CA • Millennium Biltmore Hotel

Sponsored by the ABA Criminal Justice Section and cosponsored by the Division.

Discounted registration for government, nonprofit and academics.

See **www.americanbar.org/crimjust** for agenda and registration info.

upcoming division events

Spring Executive Committee Meeting*
May 11 – 12, 2012
Des Moines, IA
***only officers are required to attend**

ABA Annual Meeting
August 3 – 5, 2012
Chicago

Division Fall Meeting
October 19 – 20, 2012
Boulder, CO

FOCUSED FORWARD
ABA 2012 Annual Meeting Chicago

Third National Conference on Employment of Lawyers with Disabilities

May 8, 2012 | Washington, DC | Wardman Marriott Park

Sponsored by the Commission on Disability Rights, cosponsored by the Division.
Discounted registration for government, nonprofit and academics.

See **www.americanbar.org/groups/disabilityrights.html** for agenda and registration info.

Kudos to Member Sharon Stern Gerstman!

Congratulations to GPSLD council member Sharon Stern Gerstman on receiving the Fellows Outstanding State Chair Award! The Fellows of the American Bar Foundation (ABF) support the research of the ABF through their annual contributions and sponsor programming of direct relevance to leaders of the legal profession. The Outstanding State Chair Award is presented annually to a Fellow who has demonstrated dedication to the work of the ABF and the mission of the Fellows through exceptional efforts at the state level.

TechTip

Greener Printing

The greenest form of printing is to not print at all. Microsoft typographer Simon Daniels advises that "the more pleasing the font looks on the screen, the less tempted someone will be to print." Times New Roman and Arial fonts are recommended for their readability.

When printing is unavoidable, testing by Printer.com reveals that some fonts use less ink than others. Century Gothic and Times New Roman were found to be the most ink efficient followed by Calibri, Verdana and Arial. Century Gothic uses about 30 percent less ink than Arial.

Want More TechTips? Visit ABA TechEZ at www.americanbar.org/groups/departments_offices/legal_technology_resources.html

MESSAGE TO THE MEMBERS

Susan Low
Chair, 2011-2012

The Division contributed greatly to the ABA Midyear Meeting in New Orleans, showcasing four exceptional programs. We are grateful to the many panelists who generously contributed their time and talents to make these programs so successful.

On Thursday, February 2, we brought our ***Public Lawyer Career Panel*** to the law students of Loyola University School of Law. The panelists—**Denise Frederick**, District Counsel, U.S. Army Corps of Engineers; **Scott Laragy**, Assistant U.S. Attorney, U.S. Attorneys' Office for the Eastern District of Louisiana; and **Sharonda R. Williams**, Chief of Litigation for the City of New Orleans—highlighted the unique professional experiences and opportunities available in public law practice.

On Friday, the Division presented three well attended and very well received CLE programs. In ***Digital Detectives: Finding Information Online Like a Pro,*** **Carole Levitt**, President, Internet for Lawyers; and **Mark Rosch**, Vice President, Internet for Lawyers; provided the audience with the most up-to-date tips and tricks of doing due diligence investigations on the internet.

E-Discovery, Public Records and Metadata: **Steve Vieux (moderator)**, Attorney, Federal Trade Commission; **David W. Degnan,** Associate, Alvarez & Gilbert, PLLC; **Wendy Muchman**, Chief of Litigation and Professional Education at the Illinois Attorney Registration and Disciplinary Commission of the Supreme Court of Illinois; **David G. Ries**, Partner, Thorp Reed & Armstrong, LLP; and **John W. Simek**, Vice President of Sensei Enterprises, Inc., provided in-depth information on this subject of direct relevance to government practitioners.

Two hours of enlightening, entertaining and audience-engaging ethics CLE credit was provided in ***Ethical Considerations in Public Sector Law***.**Gregory G. Brooker (moderator),** Assistant United States Attorney, District of Minnesota; **Paula Frederick,** General Counsel, State Bar of Georgia; **Sharon Pandak,** Partner, Greehan Taves Pandak & Stoner PLLC; **Charles B. Plattsmier,** Chief Disciplinary Counsel, Louisiana Attorney Disciplinary Board; and **William M. Ross,** Associate Professor, Tulane University; demonstrated with both humor and realism the ethical problems facing government lawyers.

We are pleased that so many could join us in New Orleans and we will continue to reach out to all our members through both live and distance learning programs. We hope that these alternative delivery methods make it easier for our members to access the resources of the Division. We plan to launch two or three additional teleconference CLE programs before the end of the bar year and would welcome your suggestions for topics and speakers for more CLE programs. If you haven't already done so, please bookmark our webpage www.governmentlawyer.org and check it often.

If you would like to become more involved in the Division or would like to see a service not currently offered, please contact me at GPSLD@americanbar.org.

By Anne Dewey-Balzhiser
President, Women Lead LLC
Former Council Member, GPSLD
Contact Anne at womenlead@cox.net

Q I was the head of a legal division of a state agency and supervised several other lawyers. However, in a recent re-structuring, I was given a different position and I no longer supervise lawyers. I consider my new position a demotion and it has really hurt my morale. Also, I think my colleagues are judging me negatively. This has been very difficult for me. Do you have any suggestions?

A Stepping down from a higher level job is never easy. I stepped down from two executive level jobs myself. When my third child was born, for example, I wanted a part-time schedule and a General Counsel's job just isn't part-time. The fact that I moved to a staff level position by my own choice didn't stop some colleagues from asking if "I miss the power" (which I frankly didn't). So, one aspect that you must deal with is the perceptions of others about what this job shift says about your competence.

It is a myth that all job changes are to higher level positions. The truth is that, especially in this fragile economy, management layers are being eliminated, resulting in downshifting of valued employees to lower level positions. Obviously, if you are able to move to a different employer, you can minimize your discomfort about how others are viewing you. Your new colleagues will likely not even know that you are now working at a different level.

Of course, that is not always possible. So, how do you bolster your morale so that you can accept—and even thrive in—your new position? Here are some suggestions. Take an inventory about what you liked and disliked about your former supervisory position and compare it to your current job. Most likely you will find that there were features of your job as a boss that you didn't enjoy, just as there are aspects of your new position which are positive.

Objectively take a good hard look at your performance evaluations in the former supervisory position. What did you do well and—more importantly—in what ways was your performance lacking? Realize that careers are long; you will have the opportunity to bolster your skills to prepare to move up later. Look for training opportunities and try to take on tasks that further develop your skills.

Finally, appreciate that each position gives one a unique perspective of the organization. I considered myself fortunate to have moved up to the top level and then moved back down. It was only when I was in a lower role again that I could view my performance as an executive more clearly. I may have thought, for example, that I was communicating well with my staff. However, when I worked for a different boss, I could see the techniques that she used and how well they worked. When I had the opportunity to take a second position in another agency as their general counsel, I had an expanded repertoire of skills to bring to the table. So hang in there. You may find that taking a break from a supervisory role is actually a positive change.

Delivery Options for Division Publications

Did you know you can now choose to receive PASS IT ON and *The Public Lawyer* via print, email or both? Simply log in to myABA at **www.americanbar.org** using your email or ABA ID number and password. Click on "subscriptions" to change your delivery options.

Division Delegate Report

By General E. E. Anderson and Darcee S. Siegel

The ABA House of Delegates held its 73rd Midyear Meeting in New Orleans on February 6, 2012. The following is a summary of House action. To see a listing of all the reports addressed by the House, visit www.americanbar.org/groups/leadership/2012_new_orleans_midyear_meeting.html (click on Daily Journal).

After welcoming remarks by New Orleans' mayor, Mitchell Landrieu, thanking the American Bar Association for having the confidence to bring the Midyear back to New Orleans, ABA President Bill Robinson III spoke about the deepening crisis of underfunding state courts. He spoke about the ABA Task Force co-chaired by Ted Olson and David Boies, created to address this problem and the great work the group is doing in highlighting this very difficult and pressing issue. He stressed that our courts are the guardians of our freedoms, the proven forum for the peaceful resolution of disputes, and the cornerstone of our constitutional democracy. As lawyers and judges—officers of the court—we have a responsibility to defend the institution that protects each of us. He further stated that as the American Bar Association, we have the responsibility to educate the public and policymakers about the essential role of our third co-equal branch of government. For an outstanding article where President Robinson addresses this crisis, see the Winter 2012 issue of the *Judges' Journal*, available at www.american bar.org/content/dam/aba/publications/judges_journal/jj_win2012.authcheckdam.pdf. We also highly recommend the excellent video that House members viewed at www.youtube.com/watch?v=wtLKAg2LRtA.

Bar Independence and Law Enforcement Access to Third Party Records

Some legislatures have sought recently to regulate the ability of state and local bar associations to function independently and freely represent the views of their members. Report 10A, which was introduced by the delegate from Puerto Rico, and which urges the highest courts or legislative bodies of all states to respect the organized bar's ability and right to function independently and express its views freely, was approved.

Resolution 101A, as amended, adopts the black letter ABA Criminal Justice Standards on Law Enforcement Access to Third Party Records. A number of other criminal justice resolutions also passed, including 101C as revised (urging judges and lawyers to consider a number of factors in weighing the use of expert testimony, such as whether the testimony of uniqueness is based on valid scientific research); 101D, (urging judges and lawyers to consider potential jurors' understanding of scientific principles relative to forensic science, as well as their preconceptions or bias with respect to such principles); 101F (supporting legislation, policies and practices that allow equal and uniform access to therapeutic courts and problem-solving sentencing alternatives); and 101G, cosponsored by the Division (urging courts to adopt written jury instructions that are in languages understandable by jurors in death penalty cases).

Cosponsored Reports

The Division cosponsored numerous resolutions, all of which were approved, some with amended language. Besides the aforementioned 101G, Resolution 105, the Model Rules for Fee Arbitration, was approved with revised language. Resolution 108 urges state and territory bar admission authorities to adopt rules that accommodate the unique needs of military spouse attorneys who cannot practice in a jurisdiction without taking a bar exam and who are required to move frequently in support of the nation's defense. It was approved with revised language. Resolution 111 urges entities that administer a law school admission test to provide appropriate accommodations for a test taker with a disability to best ensure that the exam results reflect what the exam is designed to measure and not the test taker's disability.

Resolution 113 adopts the ABA Standards for Language Access in Courts, and urges federal and state legislature and executive branches to provide funding to fully implement language access services.

Resolution 302 supports the principle that private lawyers representing governmental entities are entitled to qualified immunity from 42 U.S.C. Section 1983 claims when they are acting "under color of state law." It was approved with amended language.

Other Resolutions of Interest

After much discussion, Resolution 102B was adopted by the House; it approves the adoption of the Uniform Electronic Legal Material Act promulgated by the National Conference on Uniform State Laws in 2001.

The most debated and controversial Resolution was Resolution 103. Resolution 103 urges federal, state, territorial, tribal and local courts to consider and respect the data protection and privacy laws of any foreign sovereign, and the interests of any person who is subject to or benefits from such laws, with regard to data that is subject to preservation, disclosure or discovery. The resolution was amended to narrow the protection of data sought in discovery in civil litigation.

The late filed resolution 10B, supporting the consent jurisdiction of United States magistrate judges as being consistent with Article III of the United States Constitution, was approved without opposition.

Two other late filed Resolutions, 303 and 304 were adopted without opposition. Resolution 303 urges legislative bodies and governmental agencies to enact laws and implement policies to ensure that persons with disabilities utilizing service animals are provided access to services, programs and activities of public entities and public accommodations pursuant to the regulations implementing the American with Disabilities Act. Resolution 304 includes a clarification to the policy of distance education where, as part of the verification process, a law school must verify that the student who registers for a class is the same student that participates and takes the exam for the class.

General E. E. Anderson (U.S. Marine Corps, Ret.) was the Division's chair in 1994-1995. Darcee S. Siegel, the City Attorney of North Miami Beach, Florida was chair in 2007-2008. Both serve as Division delegates.

pass it on

American Bar Association
Government and Public Sector Lawyers Division
740 15th Street, N.W.
Washington, D.C. 20005-1022

NON-PROFIT ORGANIZATION
U.S. POSTAGE
PAID
AMERICAN BAR ASSOCIATION

AMERICAN BAR ASSOCIATION
Government and Public Sector Lawyers Division

ABA Annual Meeting

CHICAGO • AUGUST 2-7, 2012

Chicago, home of hot blues and a cool lakefront, will be the host for this year's Annual Meeting. Visit the new Modern Wing of the Art Institute or any of the other world-class museums, play with the kids at Navy Pier or take in American's greatest pastime at Wrigley Field or The Cell.

Take advantage of Early Bird Registration prices and purchase an all-access badge for $545 for admittance to governance meetings, all CLE and non-CLE programs, including those in the Presidential CLE Centre and at the satellite hotels. For members who are primarily interested in governance, a fee of $195 will allow entrance to all non-CLE programs and governance meetings.

Individual program tickets are $90 each. Discounted program tickets are available for government lawyers and judges for $35. Law student attendees will be admitted to all CLE programs at no additional charge. (Fees increase after May 31).

DEADLINE DATES

Thursday, May 31 Deadline for Early Bird Discount Rate
Friday, July 6 Deadline for Advance Registration and Housing

DIVISION SCHEDULE

Friday, August 3
5:00–6:30 p.m.
Awards Reception

Saturday, August 4
9:00–12:30 p.m.
Council Meeting and Election

Division events will take place at the Fairmont Hotel.

Please check your program book to confirm times and locations of all Annual Meeting events.

For more information or to register online, visit **www.americanbar.org/calendar/annual.html** or call the ABA Meetings and Travel Department at 312-988-5870.